# Symmetry, Reversibility, and Efficiency of Quantum Computation

Giuseppe Castagnoli*, Dalida Monti†, and Alexander Sergienko‡

(August 5, 1999)

## Abstract

The reason for the higher efficiency exhibited by some quantum algorithms over their classical counterparts is examined by considering the interplay between the reversible actions required to prepare the computer registers in an entangled state before measurement (the "initial actions"), and the final measurement action – whereas measurement is *interepreted* in a new way, particularly suited to a problem solving context. This unification shows that the computation process, comprising the measurement outcome, is significantly influenced by *both* the initial actions and the need to satisfy the constraints set by the final measurement action. Reviewing the existing quantum algorithms in the light of this *dual influence*, yields new valuable insight in the nature of the quantum computation speed up.

## I. INTRODUCTION

Understanding why some quantum algorithms are more efficient than their classical counterparts and whether such algorithms follow a common pattern is a central problem, whose

*Elsag Bailey e Università di Genova, 16154 Genova, Italy

†Elsag Bailey e Università di Genova, 16154 Genova, Italy

‡Dept. of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA

solution can potentially affect the direction of development of quantum computation. Nowadays, this problem is attracting increasing attention [1], [2].

Let us consider the evolution of a reversible quantum system which undergoes measurement with undetermined outcome: in this paper we develop a non-conventional interpretation based on this evolution being influenced by both the initial actions and the final measurement action[1]. In the case of quantum computation, this dual influence acquires a full significance and yields a valuable insight in the nature of the quantum computation speed up (i.e. the higher efficiency exhibited by quantum computation over classical computation). Of course, dual influence is a uniquely quantum feature vanishing in the classical framework, where evolutions are driven by the initial actions only or, in other words, by a sufficiently comprehensive initial condition[2].

The point we wish to make is somewhat in contrast with a frequently encountered way of thinking quantum computation. For the sake of clarity, it is convenient to make this contrast explicit. A frequent notion is: quantum computation can work in parallel on a number of inputs growing exponentially with register size, but the fact that measurement reads only one output can completely spoil this exponential wealth; however, a smart algorithm can provide an output which draws on an exponential number of computation paths. Therefore, measuring (in the sense of reading) this output keeps some of the wealth.

In the interpretation we are going to propound, measurement is not only needed to read the solution of a problem (or something useful to frame the solution). Quite the contrary,

---

[1]By "initial actions" we mean the sequence of reversible actions performed to prepare the quantum system in the state before measurement.

[2]This work has been influenced by Finkelstein's notion [3]that there are only initial and final actions, with "quantum spontaneity" (i.e. appearance of an a-priori undetermined measurement outcome) in between. In our interpretation, the special efficiency of quantum computation is hosted in this notion.

*together* with the reversible initial actions, measurement creates the solution in such a way that there is a computational speed up. As a matter of fact, given a suitable preparation, the final measurement action can be seen as an analog form of computation which, at the same time, introduces and satisfies a system of simultaneous Boolean equations representing the problem to be solved – or the hard part thereof.

To show this, we consider a quantum system made of two n-qubit registers $a$ and $v$ ($a$ for *argument*, $v$ for *value* of a function of that argument). Given $B^n = \{0,1\}^n$, $N = 2^n$, let $\mathcal{H}_{av} = span\{|x\rangle_a |y\rangle_v\}$, with $(x,y)$ running over $B^n \times B^n$, be the Hilbert space of the two registers, and

$$|\varphi, t_-\rangle_{av} = \frac{1}{\sqrt{N}} \sum_x |x\rangle_a |f(x)\rangle_v , \tag{1}$$

be the quantum state before measurement, say at time $t_-$. Here $\varphi$ labels the ket, $x$ runs over $0, 1, ..., N-1$, and $f(x)$ is a function from $B^n$ to $B^n$. We designate the binary number stored in register $a$ ($v$), a Hermitian operator, by $[a]$ ($[v]$).

Measuring $[v]$ in state (1) yields some specific eigenvalue $\overline{f} \in \{f\}$, where $\{f\}$ is the set of the eigenvalues for the measurement basis, which must cover the values assumed by $f(x)$. Correspondingly, the state of the quantum system changes to:

$$|\beta, t_+\rangle_{av} = \overline{k} \sum_x |x\rangle_a |\overline{f}\rangle_v , \tag{2}$$

where $x$ runs over all $x$ such that $f(x) = \overline{f}$ and $\overline{k} = |\overline{k}| e^{i\delta}$ is a normalization and a random phase factor (the phase factor will be understood, from now on). Although we are dealing with the evolution of the same quantum system, we have changed labels from $\varphi$ to $\beta$ to emphasize the fact that $|\beta, t_+\rangle_{av}$ is not univocally determined by $|\varphi, t_-\rangle_{av}$, for it is also influenced by the final measurement action.

In a problem solving context, it is easy to see that there is much more than a random influence. This broader influence is best shown by using a special (algebraic) representation of the usual description of quantum measurement, such that the *result* of measurement becomes the *solution* of a system of simultaneous equations applying to a ket variable be-

longing to the Hilbert space $\mathcal{H}_{av}$. This ket variable, in elementary algebra, would be called the "unknown" of the system of simultaneous equations.

Let us designate by $|\psi\rangle_{av}$ this ket variable, which is only constrained by normalization, thus:

$$|\psi\rangle_{av} = \sum_{x,y} \alpha_{xy} |x\rangle_a |y\rangle_v ,$$

where $(x, y)$ runs over $B^n \times B^n$ and $\alpha_{xy}$ are complex variables independent of each other up to $\sum_{x,y} |\alpha_{xy}|^2 = 1$. There are three equations, to be simultaneously applied to $|\psi\rangle_{av}$, whose solution is the measurement outcome $|\beta, t_+\rangle_{av}$.

i) A main constraint introduced by the action of measuring $[v]$, is that the measurement outcome must be *one single value*, namely any eigenvalue of the measurement basis. This constraint is represented by the projection equation

$$P_v |\psi\rangle_{av} = |\psi\rangle_{av} , \text{ where } P_v = |f\rangle_v \langle f|_v , \quad f \in \{f\} . \tag{3}$$

$|\psi_{av}\rangle$ satisfying eq.(3) (and the related conditions, this will be understood from now on) becomes a ket variable belonging to the Hilbert subspace $\mathcal{H}^f_{av} = span\{|x\rangle_a |f\rangle_v\}$, with $x$ running over $B^n$ and $f$ being fixed. The number of such subspaces is, of course, the number of the eigenvalues.

The fact that the measurement outcome is one single value is so natural, that it might be difficult to see it as a constraint. We should think of the action of measurement as an analog form of computation that we can choose to exploit; a significant logical constraint, to be satisfied by the measurement outcome, is introduced by this very choice. This is of course a universal constraint, holding for any initial actions, therefore *independent* of the initial actions.

ii) Provided that constraint (3) is satisfied, the following inner product

$$|\langle\psi|_{av} |\varphi, t_-\rangle_{av}| \text{ must be maximum.} \tag{4}$$

To satisfy also this constraint, $|\psi\rangle_{av}$, belonging to $\mathcal{H}^f_{av}$, must position itself in such a way that it becomes the projection of $|\varphi, t_-\rangle_{av}$ on $\mathcal{H}^f_{av}$. Together, (3) and (4) yield:

$$|\psi\rangle_{av} = k\,|f\rangle_v\,\langle f|_v\,|\varphi, t_-\rangle_{av}\,, \quad f \in \{f\}\,,$$

where $k$, depending on $f$, is a normalization factor. The operator $|f\rangle_v\,\langle f|_v$, to be applied to $|\varphi, t_-\rangle_{av}$, is also independent of the initial actions. It selects, out of the superposition $|\varphi, t_-\rangle_{av}$, all and only those tensor products containing $|f\rangle_v$, which naturally survive in the measurement outcome.

iii) The result of measuring $[v]$ must be a specific value:

$$f = \overline{f}, \tag{5}$$

where $\overline{f}$ is randomly chosen among the values of $f\,(x)$ appearing in $|\varphi, t_-\rangle_{av}$, according to their probability amplitudes. $\overline{f}$ is *partly* independent of $|\varphi, t_-\rangle_{av}$, for it is stochastically related to it. We should note that only equation (5) (and related conditions) is represented in the usual statement that the measurement outcome is random, whereas equations (3) and (4) are not.

The solution of the system of simultaneous equations (3), (4), and (5), applying to a ket variable $|\psi\rangle_{av}$ of $\mathcal{H}_{af}$, is

$$|\psi\rangle_{av} = \overline{k}\,\left|\overline{f}\right\rangle_v\,\left\langle\overline{f}\right|_v\,|\varphi, t_-\rangle_{av} = |\beta, t_+\rangle_{av}\,,$$

indeed the state after measurement of the quantum system (eq. 2).

This shows that the outcome of the computation process is determined by *both* the result of the initial actions $|\varphi, t_-\rangle_{av}$, and the requirement of satisfying a system of simultaneous constraints that are introduced by the final measurement action and are partly independent of $|\varphi, t_-\rangle_{av}$. Of course, this dual effect cannot apply to a classical evolution. Being (in principle) completely determined by an initial condition, such an evolution cannot satisfy a final constraint independent of it, disregarding the trivial case that initial condition and final

constraint are redundant with each other. How this dual influence yields the computational speed up is exemplified here below, before describing quantum algorithms in detail (Section II).

The scheme is that, by properly representing the problem to be solved in the state-before-measurement, equations (3), (4) and (5) become a system of simultaneous Boolean equations customized on the problem. Measurement, by both introducing and solving this system, produces the solution of the computationally hard part of the problem.

We shall outline the modified version [4] of Simon's algorithm [5]. Given a 2-to-1 function $f : B^n \rightarrow B^n$, such that

$$\forall x > x^{'} : f(x) = f(x^{'}) \rightarrow x = x^{'} + r \tag{6}$$

for some $r \in B^n$, and hard-to-reverse by known classical means, the problem is to find $r$ in an efficient way, which here means in poly($n$) time. By hard-to-reverse, we mean that, for all arguments $x$, computing $f(x)$ requires poly(n) time, while for all values $f$ of $f(x)$, computing the arguments $x$ and $x + r$ such that $f(x) = f(x + r) = f$ (there are two of them, given that $f$ is 2-to-1), requires exp($n$) time. In the modified Simon's algorithm, the state-before-measurement (Section II) is the superposition:

$$|\varphi, t_{-}\rangle_{av} = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle_a |f(x)\rangle_v ,$$

where $x$ ranges over $0, 1, ..., N-1$. Given the character of $f(x)$, the outcome of measuring $[v]$ has the form

$$|\beta, t_{+}\rangle_{av} = \frac{1}{\sqrt{2}} \left(|\overline{x}\rangle_a + |\overline{x} + r\rangle_a\right) \left|\overline{f}\right\rangle_v , \tag{7}$$

where $f(\overline{x}) = f(\overline{x} + r) = \overline{f}$. In Section II, we will assume that efficiency has already been achieved by preparing state (7) which, for the time being, we can consider to be "the solution".

It can be seen that measuring $[v]$ in $|\varphi, t_{-}\rangle_{av}$ brings in, through equations (3) and (4), the following constraints applying to the arguments and values of $f(x)$:

$$f(x_1) = f(x_2), \quad x_1 \neq x_2. \tag{8}$$

Since we are dealing with natural numbers, this is a succinct way of representing a system of simultaneous Boolean equations. Equation (5) becomes just the specification $f(x_1) = f(x_2) = \overline{f}$. Figure 1(a) represents this system in network form.

Fig. 1(a),(b)

The output of gate 1-2 yields the function $c : B^n \times B^n \rightarrow B$ defined as follows: $c(x_1, x_2) = 1 - \delta_{x_1,x_2}$, where $\delta$ is the Kroneker symbol. In order to have $x_1 \neq x_2$, this output must be constrained to 1. Both gates 1-3 and 2-4 transform an input $x$ into the output $f(x)$. We should keep in mind that the network shown in Fig. 1(a) is just the representation of a system of simultaneous Boolean equations: time is not involved [just like in equations (3), (4), and (5)], thus inputs and outputs loose any time-related meaning: they just stand for the arguments and the values of a function.

On the one hand, since $f(x)$ is hard-to-reverse, the Boolean network of Fig. 1(a) is hard to satisfy by classical means. As can be seen, finding a valuation of $x_1$ and $x_2$ which satisfies the network, implies reversing $f(x)$ at least once – given that gates 1-3 and 2-4 belong to a loop. This operation takes $\exp(n)$ time by assumption. On the other hand, once $|\varphi, t_-\rangle$ has been prepared, the network, no matter its computational complexity, is concurrently created and solved by the action of measuring $[v]$. A solution, a proper valutation of $x_1$ and $x_2$, is represented in the quantum superposition (7) ($r$ can "easily" be extracted from this superposition – Section II). Since $|\varphi, t_-\rangle$ is prepared in poly(n) time, there is an exponential speed up,

Network topology is relevant, given that computational hardness comes from the loop of conditional logical implications appearing in Fig. 1(a)[3]. The capability of satisfying this

[3]By a conditional logical implication we mean, for example: *if* the input is $\underline{x}$, *then* the output is $f(\underline{x})$, etc.

loop in one shot belongs to the character of quantum measurement and traces back to the projection equation (3), whose network representation is naturally a loop – Fig. 1(b) (wires mean identity).

Thus, given proper initial actions, quantum measurement can be seen as an *analog form of computation*, capable of satisfying a system of simultaneous Boolean equations in one shot. It is a special form of analog computation. Generally speaking, (any) analog computation implies some sort of identification between the mathematical definition of an object and its physical determination. The object can be either a process or a result (i.e. the solution of a problem).

In problem solving, the problem *implicitly* defines its solution. In order to construct the solution by classical means, an implicit definition must first be made explicit, or constructive, in other words it must be changed into an algorithm. This should also hold for classical analog computation, under the assumption that it can always be efficiently simulated by an algorithm.

Going back to the quantum case, the foregoing system of simultaneous Boolean equations defines its solutions in a highly implicit way. Therefore, quantum analog computation is non-classical as far as it yields identification between *implicit* (*algebraic*) *definition* of an object and its *physical determination*. Here the object is a solution satisfying the system. If one steeks to the classical notion of algorithm, it can be said that "quantum algorithms" comprise a non-algorithmic part.

Interestingly, this quantum capability of solving algebraic equations, is not unique to quantum computation. In the case of the discrete spectrum, eigenvalues are, of course, the solutions of the algebraic equation obtained by setting to zero the determinant of a homogeneous system of linear equations. Measurement, yielding one of such eigenvalues, analagously computes a solution of the equation. This appears to be a potentially interesting "unification" between quantum computation and the most traditional quantum mechanics.

In the following Sections, we will test our model on a variety of efficient quantum algorithms; we will follow the unified version of these algorithms given by Cleve et al. [4]. Finally,

we should like to mention previous explorative work on the dual influence paradigm: [10], [11], [12].

## II. SIMON'S AND SHOR'S ALGORITHM

Given a hard-to-reverse function $f : B^n \rightarrow B^n$, such that it satisfies condition (6), both Simon's algorithm [5], as modified in [4], and Shor's algorithm [6] deal with the problem of finding $r$ in an efficient way.

### A. Modified Simon's algorithm

In order to make our point more visible, we will follow a simplified/introductory version [4] of Simon's algorithm. With respect to the original version, we must confine ourselves to the case that the oracle gives us a 2-to-1 function $f : B^n \rightarrow B^n$ such that

$$\forall x \neq x^{'} : f\left(x\right) = f(x^{'}) \Longleftrightarrow x = x^{'} \oplus r,$$

where $\oplus$ denotes bitwise exclusive or. The problem is to find $r$ in poly(n) time. With a further simplification, as anticipated in Section I, we replace the above condition with condition (6).

Instead of being computed by a black box (oracle), the function can simply be thought of as being hard-to-reverse by known classical means. In this way, we will also capture the main feature of Shor's algorithm: finding the period $r$ of a hard-to-reverse function. The following table gives a trivial example.

| $x$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $f\left(x\right)$ | 0 | 1 | 0 | 1 |

Table I

The modified algorithm is given in Fig. 2 – we should disregard $/F$ for the time being.

Fig. 2

Registers $a$ and $v$ undergo successive unitary transformations, either jointly or separately:

- The $f(x)$ transform (a reversible Boolean gate in the time-diagram of computation – Fig. 3) leaves the content of register $a$ unaltered, so that an input $x$ is repeated in the corresponding output, and computes $f(x)$ adding it to the former content of register $v$ (which was set to zero). If the state is not sharp but is a quantum superposition, the same transformation applies to any tensor product appearing in the superposition.

Fig. 3

- $H$ is the Hadamard transform. On a single qubit $i$, it operates as follows: $|0\rangle_i \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle_i + |1\rangle_i)$, $|1\rangle_i \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle_i - |1\rangle_i)$. In the general case of a register of n qubits, containing the number $\overline{x}$, it yields $|\overline{x}\rangle_a \xrightarrow{H} \frac{1}{\sqrt{N}}\sum_x (-1)^{\overline{x}\cdot x}|x\rangle_a$, where $N = 2^n$, $x$ ranges over $0, 1, ..., N-1$, and $\overline{x}\cdot x$ denotes the module 2 inner product of the two numbers in binary notation (they should be seen as row matrices). Of particular interest is the transformation $|0\rangle_a \xrightarrow{H} \frac{1}{\sqrt{N}}\sum_x |x\rangle_a = \frac{1}{\sqrt{N}}(|0\rangle_a + |1\rangle_a + ... + |N-1\rangle_a)$, which will be used to prepare register $a$ in an even superposition of all possible values of the argument.

- $M$ represents the action of measuring the binary content of a register; on register $a$, it operates as follows: $M|x\rangle_a = x|x\rangle_a$, and similarly for $v$.

The modified Simon's algorithm proceeds through the following actions (applied to table I example); each point gives the action and the corresponding result:

a) prepare:

$|\varphi, t_0\rangle_{av} = |0\rangle_a |0\rangle_v$;

this is obtained by applying an appropriate unitary transformation to the result of an initial measurement of all qubits;

b) perform the Hadamard transform on register $a$ :

$|\varphi, t_1\rangle_{av} = \frac{1}{\sqrt{N}} \sum_x |x\rangle_a |0\rangle_v = \frac{1}{2} (|0\rangle_a |0\rangle_v + |1\rangle_a |0\rangle_v + |2\rangle_a |0\rangle_v + |3\rangle_a |0\rangle_v)$ ;

c) compute $f(x)$, add result to the former content (0) of register $v$ :

$|\varphi, t_2\rangle_{av} = \frac{1}{\sqrt{N}} \sum_x |x\rangle_a |f(x)\rangle_v = \frac{1}{2} (|0\rangle_a |0\rangle_v + |1\rangle_a |1\rangle_v + |2\rangle_a |0\rangle_v + |3\rangle_a |1\rangle_v)$ ;

this is the state before measurement;

d) measure $[v]$, thus obtaining, say, the eigenvalue $\overline{f} = 1$; the state after measurement is then:

$|\beta, t_3\rangle_{av} = \frac{1}{\sqrt{2}} (|\overline{x}\rangle_a + |\overline{x} + r\rangle_a) |\overline{f}\rangle_v = \frac{1}{\sqrt{2}} (|1\rangle_a + |3\rangle_a) |1\rangle_v$ ,

We should note that it is *equivalent* to either perform or skip $[v]$ measurement (see further below). It will be easier to understand the algorithm if we assume that the measurement has been performed. The measurement outcome $|\beta, t_3\rangle_{av} = \sqrt{\frac{N}{2}} |\overline{f}\rangle_v \langle\overline{f}|_v |\varphi, t_2\rangle_{av}$ is naturally dually influenced (Section I).

Ekert and Jozsa [1] have shown that quantum entanglement between qubits is essential for providing computational speed up, in terms of time *or* resources, in the class of quantum algorithms we are dealing with (which yield exponential speed up). After measuring $f(x)$, the state of the two registers becomes factorizable, and all entanglement is destroyed. The remaining actions, performed on register $a$, use interference (which generates no entanglement) to "extract" $r$ out of the superposition $\frac{1}{\sqrt{2}} (|\overline{x}\rangle_a + |\overline{x} + r\rangle_a)$. We conclude that the computational speed up has already been achieved by preparing $|\beta, t_3\rangle_{av}$.

e) perform $H$ on register $a$ :

$|\beta, t_4\rangle_{av} = \frac{1}{\sqrt{2N}} \sum_z (-1)^{\overline{x} \cdot z} [1 + (-1)^{r \cdot z}] |z\rangle_a |\overline{f}\rangle_v$;

f) measure $[a]$ in $|\beta, t_4\rangle_{av}$; we designate the result by $z$;

$r \cdot z$ must be 0 – see the form of $|\beta, t_4\rangle_{av}$;

g) by repeating the overall computation process a sufficient number of times, poly($n$) on average, a number of constraints $r \cdot z = 0$ sufficient to identify $r$ is gathered.

Let us see how speed up is achieved in the time-interval $[t_1, t_3]$ involving generation of entanglement and quantum measurement. There are two interpretations.

$\mathcal{A}$) The first one has been anticipated in Section I. The final action of measuring $[v]$ in state $|\varphi, t_2\rangle_{av}$, at the same time creates the system of simultaneous Boolean equations (8) and yields a quantum superposition representing the values of $x_1$ and $x_2$ which satisfy the system ($r$ is "easily" extracted from this superposition). Achieving an equivalent result in classical computation would require exp($n$) time.

$\mathcal{B}$) A second interpretation focuses on computation reversibility. Speed up comes from running the direct function computation back in time, in a completely symmetrical way starting from the measurement outcome as though it were an initial state.

This can be illustrated by resorting to time symmetrized quantum measurement [7], [8]. Here, the evolution of the quantum system in $[t_1, t_3]$, is represented by means of *two* unitary evolutions:

- one is the usual evolution of the ket $|\varphi, t\rangle_{av} = U(t, t_1)\,|\varphi, t_1\rangle_{av}$, with $t_2 \geqslant t \geqslant t_1$, which starts from $t_1$ and deterministically ends into the state before measurement $|\varphi, t_2\rangle_{av}$;
- the other is the evolution of the ket $|\beta, t\rangle_{av}$. By definition, this ket undergoes the same unitary transformations of $|\varphi, t\rangle_{av}$, but deterministically ends into the result of measurement $|\beta, t_3\rangle_{av}$. In other words, $|\beta, t\rangle_{av}$ starts from $|\beta, t_3\rangle_{av}$ and goes back in time undergoing, in reverse, the same transformations of the forward evolution: $|\beta, t\rangle_{av} = U^{\dagger}(t_3, t)\,|\beta, t_3\rangle_{av}$, with $t_1 \leqslant t \leqslant t_3$. Thus

$$|\beta, t_3\rangle_{av} = |\beta, t_2\rangle_{av} = \frac{1}{\sqrt{2}}\left(|\overline{x}\rangle_a + |\overline{x} + r\rangle_a\right)\left|\overline{f}\right\rangle_v = \frac{1}{\sqrt{2}}\left(|1\rangle_a + |3\rangle_a\right)|1\rangle_v$$

$$|\beta, t_1\rangle_{av} = \frac{1}{\sqrt{2}} \left( |\overline{x}\rangle_a + |\overline{x} + r\rangle_a \right) |0\rangle_v = \frac{1}{\sqrt{2}} \left( |1\rangle_a |0\rangle_v + |3\rangle_a |0\rangle_v \right), \tag{9}$$

Evidently $|\beta, t\rangle_{av}$, like its outcome $|\beta, t_3\rangle_{av}$, is simultaneously determined by both the result of the initial actions and the final measurement action.

For the sake of explanation, it is useful to resort to the notion of "wave function collapse" which here means switching, at some time $t$, from $|\varphi, t\rangle_{av}$ to $|\beta, t\rangle_{av}$[4]. According to von Neumann, Wigner et al., collapse can be back-dated to any time during the unobserved, reversible life of the quantum system between initial and final measurement.

To the purpose of the current interpretation, it is convenient to place collapse at time $t_1$, immediately before direct function computation. Accordingly, at $t_1$, the evolution switches from $|\varphi, t_1\rangle_{av}$ to $|\beta, t_1\rangle_{av}$ [step (b) and equation (9), respectively]. In other words, the state of register $a$ (as in $|\varphi, t_1\rangle_{av}$) collapses on the superposition $\frac{1}{\sqrt{2}} \left( |\overline{x}\rangle_a + |\overline{x} + r\rangle_a \right) = \frac{1}{\sqrt{2}} \left( |1\rangle_a + |3\rangle_a \right)$. This is the superposition of the two arguments such that their function, computed afterwards, will be $\overline{f}$. This is *equivalent* to having computed the reverse function in the same time-interval $[t_1, t_2]$ taken to compute the direct function. Hence the higher than classical efficiency, since the time taken is poly$(n)$ rather than exp$(n)$.

We should note that this does not imply that computation goes back in time as though the direction of causality went back in time, but it strictly implies computation reversibility. Hence, the direction of causality can be disregarded, provided that the states of the quantum system at different times "match", according to the initial condition, the final measurement, and the unitary propagations in between.

Of course, also interpretation $\mathcal{A}$ implies computation reversibility. It is indeed based on the assumption of performing a measurement in a coherent quantum superposition that

---

[4]It should be noted that collapse is not needed in any essential way: we are just free to choose to either introduce or not introduce it. Introducing it facilitates the discussion, exactly as in the case of point (d).

represents the outputs of a computation and the memory of the corresponding inputs. This coherent superposition is necessarily generated by a *reversible* computation process which starts from the result of an initial measurement of all qubits.

In conclusion, both interpretations involve reversible computation and quantum measurement in an inseparable way – inseparable (it can be argued) in the sense of Bohr's complementarity principle.

Finally, let us show that performing or skipping step (d) (i.e. $[v]$ measurement at time $t_2$) is *equivalent*. We will follow a shortcut. Let us skip step (d) and measure $[a]$ first, at time $t_4$. In Fig. 2, $M$ on $v$ should be shifted at least after $t_5$. Whether $[v]$ is measured after $t_5$ is indifferent. Let us think of measuring it. This induces a wave function collapse of the state of register $v$ on some $\left|\overline{f}\right\rangle_v$. Since $\left|\overline{f}\right\rangle_v$ is disentangled from the state of register $a$, and no operation is performed on register $v$ after time $t_2$, back-dating collapse at time $t_2$ means back-dating the result of collapse ($\left|\overline{f}\right\rangle_v$) as it is. This is equivalent to having performed step (d).

### B. Shor's algorithm

The problem of factoring an integer $L$ – the product of two unknown primes – is transformed into the problem of finding the period of the function $f(x) = a^x \bmod L$, where $a$ is an integer between 0 and $L-1$, coprime with $L$ [9]. Figure 2 can also represent Shor's algorithm, provided that $f(x)$ is defined as above and that the second Hadamard transform is substituted by the discrete Fourier transform $F$. The state before measurement still has the form $|\varphi, t_2\rangle_{av} = \frac{1}{\sqrt{L}} \sum_x |x\rangle_a |f(x)\rangle_v$. Measuring or not measuring $f(x)$ in $|\varphi, t_2\rangle_{av}$ is still equivalent. By measuring it, the above state collapses on the superposition

$$\overline{k} \left(|\overline{x}\rangle_a + |\overline{x}+r\rangle_a + |\overline{x}+2r\rangle_a + ...\right) \left|\overline{f}\right\rangle_v, \tag{10}$$

where $f(\overline{x}) = f(\overline{x}+r) = ... = \overline{f}$ and $\overline{k}$ is a normalization factor.

The second part of the algorithm generates no entanglement and serves to "extract" $r$, by using Fourier-transform interference and auxiliary, off line, mathematical considerations. Un-

der the current assumptions, quantum computation speed up has been achieved by preparing state (10): the discussion is completely similar to that of the previous algorithm.

## III. QUANTUM ORACLE COMPUTING

Until now we have faced the problem of efficiently reversing a hard-to-reverse function $f(x)$. All the knowledge of the problem and ignorance about the solution have been physically represented in an entangled state like $|\varphi, t_-\rangle_{av}$ (eq. 1). In the language of game theory, these are games against (mathematical) nature.

Quantum oracle computing is better seen as a competition between two players. One prepares the problem and either knows the solution or has a privileged access to it. The other one knows the problem, not the solution, and has no privileges: she/he must find the solution in the most efficient way.

Sticking to Greek tradition, we shall call the former player Sphinx, the latter Oedipus. The game is formalized as follows. Both players know everything of a set of software programs $\{f_k\}$, whereas each program $f_k$ computes some function $f_k : B^n \to B^n$. The Sphinx chooses $k$ at random, loads program $f_k$ on a computer (i.e., sets the oracle in its $k$-th mode) and passes it on to Oedipus. Oedipus knows nothing of the Sphinx' choice and must efficiently find $k$ by testing the computer (oracle) input-output behaviour. If the computer is quantum, then we speak of "quantum oracle computing".

### A. Deutsch's 1985 algorithm

$\{f_k\}$ is the set of all possible functions $f_k : B \to B$, namely:

| $x$ | $f_{00}(x)$ |
|---|---|
| 0 | 0 |
| 1 | 0 |

| $x$ | $f_{01}(x)$ |
|---|---|
| 0 | 0 |
| 1 | 1 |

| $x$ | $f_{10}(x)$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

| $x$ | $f_{11}(x)$ |
|---|---|
| 0 | 1 |
| 1 | 1 |

$\{f_k\}$ is divided into a couple of subsets: the balanced functions, characterized by an even number of zero and one values, thus labeled by $k = 01, 10$, and the unbalanced ones, labeled by $k = 00, 11$. Once set in its $k$-th mode, the oracle computes $f_k(x)$. Oedipus must find whether the oracle (whose mode has been randomly set by the Sphinx) computes a balanced or an unbalanced function, with a minimum number of oracle runs. Deutsch's algorithm, as modified in [4] is represented in Fig. 4(a). The computation of $f_k(x)$ is represented by a reversible Boolean gate like in the previous algorithms, but for the fact that the result of computation has now to be module 2 added to the former content of register $v$.

Fig. 4(a),(b)

The algorithm proceeds as follows; each point gives the action and the corresponding result.

a) prepare:

$$|\varphi_k, t_0\rangle_{av} = \tfrac{1}{\sqrt{2}} |0\rangle_a (|0\rangle_v - |1\rangle_v),$$

b) perform the Hadamard transform on register $a$:

$$|\varphi_k, t_1\rangle_{av} = \tfrac{1}{2} (|0\rangle_a + |1\rangle_a) (|0\rangle_v - |1\rangle_v),$$

c) we shall consolidate the next two steps – Fig. 4(a): compute $f_k(x)$, module 2 add the result to the former content of register $v$, perform the Hadamard transform on register $a$; we must distinguish for the different values of $k$:

$$|\varphi_{00}, t_3\rangle_{av} = \tfrac{1}{\sqrt{2}} |0\rangle_a (|0\rangle_v - |1\rangle_v)$$

$$|\varphi_{01}, t_3\rangle_{av} = \tfrac{1}{\sqrt{2}} |1\rangle_a (|0\rangle_v - |1\rangle_v)$$

$$|\varphi_{10}, t_3\rangle_{av} = -\tfrac{1}{\sqrt{2}} |1\rangle_a (|0\rangle_v - |1\rangle_v)$$

$$|\varphi_{11}, t_3\rangle_{av} = -\tfrac{1}{\sqrt{2}} |0\rangle_a (|0\rangle_v - |1\rangle_v)$$

d) measure the content of register $a$: it can be seen that obtaining 1 (0) means that the function is balanced (unbalanced). In other words, the result of measurement yields the characteristic function of the balanced function (or mode).

This algorithm is more efficient than any classical algorithm, where two runs of the oracle are required to find the mode. However, the result is apparently reached in a deterministic way, without any dual influence on the computation process.

This can be ascribed to an incomplete physical representation of the problem. Not only the computation of the solution, but also the definition of the problem should be physically represented[5]. From another perspective, Oedipus is not independent of the Sphinx. To have a closed system, we must consider both.

This is readily done by introducing the extended gate $F(k,x)$ which computes the function $F(k,x) = f_k(x)$ for all $k$ and $x$; the gate has an ancillary input register $m$ ($m$ for mode) which contains $k$, i.e. the oracle mode. This input is identically repeated in a corresponding output (to keep gate reversibility). Figure 4(b) gives the extended algorithm. Of course, Oedipus is forbidden to access register $m$. The preparation becomes

$$|\varphi, t_0\rangle_{mav} = \frac{1}{\sqrt{2}} |0\rangle_m |0\rangle_a (|0\rangle_v - |1\rangle_v).$$

After performing Hadamard on $m$ and $a$ we obtain:

$$|\varphi, t_1\rangle_{mav} = \frac{1}{4} (|00\rangle_m + |01\rangle_m + |10\rangle_m + |11\rangle_m) (|0\rangle_a + |1\rangle_a) (|0\rangle_v - |1\rangle_v). \tag{11}$$

Performing Hadamard on $|0\rangle_m$ is a way of representing Oedipus' ignorance about the Sphinx' choice. Let us go directly to the state before the first measurement – see Fig. 4(b)

$$|\varphi, t_3\rangle_{mav} = \frac{1}{2\sqrt{2}} [(|00\rangle_m - |11\rangle_m) |0\rangle_a + (|01\rangle_m - |10\rangle_m) |1\rangle_a] (|0\rangle_v - |1\rangle_v). \tag{12}$$

By measuring $[a]$ and $[m]$ in any order, the content of register $a$ gives the "characteristic function" $c(k)$ of the balanced mode [$c(k) = 1$ for balanced, $c(k) = 0$ for unbalanced], as can be seen.

With the extended algorithm, the competition can follow two alternative protocols.

---

[5]In Section II, all knowledge of the function and ignorance about $r$ were physically represented in a superposition of the form (1).

A) First the Sphinx measures $[m]$ and finds, say, 01. Concurrently, $|\varphi, t_3\rangle_{mav}$ (eq. 12) has collapsed on

$$|\beta, t_4\rangle_{mav} = \frac{1}{\sqrt{2}} |01\rangle_m |1\rangle_a (|0\rangle_v - |1\rangle_v) ,$$

$k = 01$ becomes the random choice performed by the Sphinx[6]. Oedipus then measures $[a]$ in $|\beta, t_4\rangle_{mav}$ and finds 1. He declares that the mode is balanced and the Sphinx sees that the answer is correct.

B) This second protocol exemplifies the irrelevance of time ordering the two measurements – in Fig. 4(b) this ordering should be inverted. First Oedipus measures $[a]$ finding, say, 1. Correspondingly, $|\varphi, t_3\rangle_{mav}$ (eq. 12) has collapsed on a new $|\beta, t_4\rangle_{mav}$:

$$|\beta, t_4\rangle_{mav} = \frac{1}{2} (|01\rangle_m - |10\rangle_m) |1\rangle_a (|0\rangle_v - |1\rangle_v) ,$$

Oedipus declares that the mode is balanced. The Sphinx measures $[m]$ (inducing a further collapse) finding, say, 01, anyhow checking that Oedipus' answer is right. However, the order of the two collapses can be inverted by backdating the second one. This brings us back to protocol $A$. The two protocols are equivalent. Resorting to both will facilitate exposition.

Let us follow protocol $A$ and see the role played by equations (3), (4) and (5) introduced by the Sphinx' action of measuring $[m]$ in state (12).

In the first place, they serve to *complete* the physical representation of the problem. Given the form of $|\varphi, t_3\rangle_{mav}$, equations (3) and (5) represent the random choice of one oracle mode performed by the Sphinx. Say it comes out $k = 01$.

---

[6]Collapse can be back-dated at time $t_1$, which can be before the Sphinx gave the oracle to Oedipus. Without entering into detail, we obtain: $|\beta, t_1\rangle_{mav} = \frac{1}{2} |01\rangle_m (|0\rangle_a + |1\rangle_a) (|0\rangle_v - |1\rangle_v)$ . This brings us to the original protocol back again – compare with $|\varphi_k, t_1\rangle_{av}$, point (b) of this Section. The only difference is that the definition of the problem has been represented.

In the second place, constraint (4) makes the state of register $a$ collapse on $|1\rangle_a$, thus changing entanglement into properly correlated measurement outcomes. Therefore, the Sphinx' action selects the oracle mode and the problem solution at the same time. Then, Oedipus measures $[a]$ finding 1, without inducing any further collapse.

This is more dramatically rendered by following the equivalent protocol $B$. Oedipus' action of measuring $[a]$, at the same time yields the solution (say it is $1 \equiv$ balanced) and selects a superposition of balanced oracle modes, $\frac{1}{\sqrt{2}}(|01\rangle_m - |10\rangle_m)$, consistent with the solution.

In other words, producing the solution of the problem, simultaneously (at the same time) selects the definition of the problem in such a way that the solution is right. Here, dual influence becomes the mutual physical definition (see Section I) of the problem and its solution; and this turns out to be more efficient than any classical computation. This is something clearly impossible to achieve in the classical framework, where the definition of the problem must be "propagated" to the solution of the problem by means of some algorithm.

This time, the "Boolean equation" (see Section I) at the same time introduced and satisfied by measuring either $[m]$ or $[a]$ in state (12), is

$$x = c(k),$$

where $x$ is the content of register $a$ and $k$ is the content of register $m$ (we should keep in mind that $c(k)$ is the characteristic function of the balanced mode). Variables $x$ and $k$ are not separately defined before measurement, given that their values are represented in an entangled way in (12). After measurement, they become separately defined and properly correlated.

It should be noted that the current Boolean equation does not imply any loop of conditional logical implication. We have seen that solving such a loop can give an exponential speed up. The seminal Deutsch's algorithm we are dealing with, cannot by itself be positioned in a complexity class (of course, problem size is not a variable if we have only one

problem). However, roughly speaking, we can say that its computational complexity is lower with respect to Simon's and Shor's problems.

This will become clearer by considering also an instance of Grover's algorithm (Section III B), where the system of Boolean equations has the same open form.

Finally, we should note a curiosity: in the context of quantum oracle computing, quantum computation proves to be, so to speak, "contagious". In order to physically represent both the problem and the solution algorithm, Oedipus' uncertainty about (possibly) classical events must be represented in a quantum way. As a matter of fact, the Sphinx could choose the oracle mode by tossing a classical coin twice, but the result is *by definition* unobservable to Oedipus. He just knows that there are four possible mutually exclusive, evenly probable results. In order to represent Oedipus' state of uncertainty, in such a way that it correctly interplays with the quantum algorithm, we must use a quantum superposition like $\frac{1}{2}\left(\left|00\right\rangle_m + \left|01\right\rangle_m + \left|10\right\rangle_m + \left|11\right\rangle_m\right)$ – see eq. (11) (the notion that the Sphinx performs a random choice is then represented by the action of measuring $[m]$).

There is an evident analogy with the usual description of quantum measurement where, at a certain stage, the position of the classical pointer must be described in a quantum way.

### B. An instance of Grover's algorithm

This time we have the set of the $2^n$ functions $f_k : B^n \rightarrow B$ such that $f_k\left(x\right) = \delta_{k,x}$, where $\delta$ is the Kroneker symbol. We shall limit ourselves to considering the simplest instance $n = 2$. This yields four functions $f_k\left(x\right)$, labeled by $k = 0, 1, 2, 3$. Figure 5(a) gives Grover's algorithm for $n = 2$. Let us assume the Sphinx has chosen $k = 2$. The preparation is $\frac{1}{\sqrt{2}}\left|0\right\rangle_a\left(\left|0\right\rangle_v - \left|1\right\rangle_v\right)$. Without entering into detail, the state before measurement is: $\frac{1}{\sqrt{2}}\left|2\right\rangle_a\left(\left|0\right\rangle_v - \left|1\right\rangle_v\right)$. Measuring $[a]$ deterministically yields the result we are looking for. This is more efficient than classical computation where three oracle runs are required to find the solution with certainty, whereas in Grover's algorithm two runs are enough – Fig. 5(a).

Fig. 5(a),(b)

The extended algorithm is given in Fig. 5(b). The preparation becomes $\frac{1}{\sqrt{2}}|0\rangle_m|0\rangle_a(|0\rangle_v - |1\rangle_v)$; the state before measurement becomes: $\frac{1}{2\sqrt{2}}(|0\rangle_m|0\rangle_a + |1\rangle_m|1\rangle_a + |2\rangle_m|2\rangle_a + |3\rangle_m|3\rangle_a)(|0\rangle_v - |1\rangle_v)$. Measuring $[a]$ yields the value of the mode and selects the mode at the same time, as in the previous oracle problem.

## IV. CONCLUSIONS

We have shown that the speed up of quantum algorithms implies that such algorithms are symmetrically influenced at both ends: by the reversible initial actions, required to prepare the system in the state before measurement, and by the final measurement action. This dual influence (apparently, an up-to-date illustration of Bohr's complementarity principle) is an exclusively quantum feature which acquires full significance in the context of quantum computation.

On the one side, this work corroborates the idea that quantum computation can shed light on the fundamental features of quantum mechanics. On the other side, we have broadened our insight in the nature of the quantum computation speed up. This might turn out to be valuable in developing quantum computation.

## V. ACKNOWLEDGEMENTS

Thanks are due to T. Beth, A. Ekert, D. Finkelstein and V. Vedral for their stimulating discussions and valuable comments on this and other related works.

# REFERENCES


[1] A. Ekert, R. Jozsa, quant-ph/9803072, to appear in Phil. trans. Roy. Soc. (Lond.) 1998, Proc. of Roy. Soc. Discussion Meeting, Nov. 97.

[2] A.Yu. Kitaev, quant-ph/9707021.

[3] D. Finkelstein, *Quantum Relativity* (Springer, Berlin Heidelberg 1996).

[4] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, quant-ph/9708016, submitted to Proc. Roy. Soc. Lond. A.

[5] D.R. Simon, *Proc. of the $35^{th}$ Annual Symposium on the Foundation of Computer Science*, Santa Fe, IVM (1994).

[6] P. Shor, *Proc. of the $35^{th}$ Annual Symposium on the Foundation of Computer Science*, Los Alamitos, **CA**, 124 (1994).

[7] A. Aharanov, P. Bergmann, J. Lebowitz, Phys. Rev. B **134**, 1410 (1964).

[8] L. Vaidman, quant-ph/9807075, to appear in PSA 98.

[9] R. Cleve, A. Ekert, L. Henderson, C. Macchiavello, M. Mosca, quant-ph/9903061, Complexity **4**, 33 (1998).

[10] G. Castagnoli, quant-ph/9902027.

[11] G. Castagnoli, D. Monti, quant-ph/9811039, submitted to Proc. of the International Quantum Structures Association Conference, Liptovsky Jan, Sept. 98.

[12] G. Castagnoli, Physica D **120**, 48 (1998).